ФОРМУЛЫ ОГРАНИЧЕННОЙ ГЛУБИНЫ В БАЗИСЕ $\{8, \oplus\}$ И НЕКОТОРЫЕ КОМБИНАТОРНЫЕ ЗАДАЧИ

А. А. Разборов

(Москва)

В работе с помощью булевых функций кодируются комбинаторные объекты (графы, турниры и т. д.), размер которых экспоненциален от числа переменных функции. В ряде случаев доказывается существование формул ограниченной глубины полиномиального размера в базисе $\{\&, \oplus\}$, которые кодируют комбинаторные объекты, обладающие заданными свойствами.

ВВЕДЕНИЕ

С помощью булевых функций можно естественным образом кодировать комбинаторные объекты (графы, турниры и т. д.), размер которых экспоненциален от числа переменных функции. Например, функция $f(x_1, \ldots, x_n, \ldots, x_{2n})$ от $2n$ переменных кодирует двудольный граф $H(f)$ с долями $\{0, 1\}^n$ и $\{0, 1\}^n$ по правилу $\langle \varepsilon, \delta \rangle \in H(f) \Leftrightarrow f(\varepsilon, \delta) = 1$. Работа посвящена изучению взаимосвязей между сложностью функции f и свойствами объекта, соответствующего ей при этих кодированиях. В несколько другой плоскости эти вопросы рассматривались в [6].

Более точно, мы показываем существование булевых функций, вычислимых с помощью функциональных схем полиномиального размера и кодирующих комбинаторные объекты, которые обладают заданными свойствами. Фактически мы используем функциональные схемы очень специального вида — это формулы глубины не более пяти в базисе $\{\&, \oplus\}$. Для сравнения отметим, что даже некоторые симметрические булевы функции не могут быть реализованы схемами (а, значит, и формулами) ограниченной глубины полиномиального размера в базисе $\{\&, \oplus\}$ ([1, 7, 5]).

Почти все рассматриваемые нами примеры взяты из книги [2]. К их числу относятся, например, следующие:

а) неориентированный граф G на N вершинах не содержит полного подграфа размера $2\log_2 N$, и то же самое справедливо для его дополнения (теорема 1 ниже);

б) для любых $(1 - o(1))\log_2 N$ игроков турнира T, в котором всего участвует N игроков, найдётся игрок, выигравший у них (теорема 5).

При доказательстве предлагаемых теорем существенно используется вероятностный метод. Поэтому наши доказательства не дают возможности явно предъявить примеры формул, су-

ществование которых мы утверждаем. Нахождение таких примеров представляется интересной и, по-видимому, трудной задачей.

В § 1 вводятся некоторые определения, касающиеся булевых функций, и доказывается несколько технических лемм. В § 2 мы доказываем существование искомых формул.

§ 1. ВСПОМОГАТЕЛЬНЫЕ ЛЕММЫ

Пусть $B_n \rightleftharpoons \{0, 1\}^n$; $G_n \rightleftharpoons \{0, 1\}^{B_n}$ — семейство всех n — местных булевых функций от n булевых переменных $x_1, \ldots, x_n$. Через $\oplus$ обозначается операция сложения по mod 2. Определение формулы глубины k в базисе $\{\&, \oplus\}$ даётся индукцией по k. *Формула глубины* 0 есть, по определению, элемент множества $\{x_1, x_2, \ldots, x_n, 0, 1\}$. *Формулой глубины* k (в базисе $\{\&, \oplus\}$) называется выражение вида $\overset{t}{\underset{i=1}{*}} F_i$, где F_i — формулы глубины $(k-1)$, а $*$ обозначает $\&$, если k чётно и $\oplus$, если k нечётно. Через $f(F)$ будем обозначать булеву функцию f, вычисляемую формулой F; *размером* $s(F)$ формулы F назовём число вхождений неизвестных в F.

Пусть теперь m, r, l — натуральные числа. Обозначим через $\mathfrak{M}(n, m, r)$ множество всех формул глубины три, которые имеют следующий вид:

$$\bigoplus_{\alpha=1}^{r} \&_{\beta=1}^{m} \bigoplus_{\gamma=1}^{n} (\lambda_{\alpha\beta\gamma} x_\gamma \oplus \lambda_{\alpha\beta}), \tag{1}$$

где $\lambda_{\alpha\beta}$; $\lambda_{\alpha\beta\gamma} \in \{0, 1\}$. Очевидно, $\forall F \in \mathfrak{M}(n, m, r)$ $(s(F) \leqslant nmr)$. Аналогично, через $\mathfrak{M}(n, m, r, l)$ обозначим множество формул глубины четыре в базисе $\{\&, \oplus\}$ вида

$$\&_{i=1}^{l} \bigoplus_{\alpha=1}^{r} \&_{\beta=1}^{m} \bigoplus_{\gamma=1}^{n} (\lambda_{i\alpha\beta\gamma} x_\gamma \oplus \lambda_{i\alpha\beta}). \tag{2}$$

Тогда $\forall F \in \mathfrak{M}(n, m, r, l)\,(s(F) \leqslant nmrl)$.

Рассмотрим теперь случайные формулы $\mathbf{F}(n, m, r)$ и $\mathbf{F}(n, m, r, l)$, которые равномерно распределены на множествах $\mathfrak{M}(n, m, r)$ и $\mathfrak{M}(n, m, r, l)$ соответственно. Тогда

$$\mathbf{F}(n, m, r) = \bigoplus_{\alpha=1}^{r} \&_{\beta=1}^{m} \bigoplus_{\gamma=1}^{n} (\lambda_{\alpha\beta\gamma} x_\gamma \oplus \lambda_{\alpha\beta}), \tag{3}$$

где $\{\lambda_{\alpha\beta}, \lambda_{\alpha\beta\gamma}\}$ — совокупность из $(n+1)mr$ независимых, равномерно распределенных на $\{0, 1\}$ случайных величин. Аналогично,

$$\mathbf{F}(n, m, r, l) = \&_{i=1}^{l} \bigoplus_{\alpha=1}^{r} \&_{\beta=1}^{m} \bigoplus_{\gamma=1}^{n} (\lambda_{i\alpha\beta\gamma} x_\gamma \oplus \lambda_{i\alpha\beta}). \tag{4}$$

Положим теперь $\mathbf{f}(n, m, r) = f(\mathbf{F}(n, m, r))$; $\mathbf{f}(n, m, r, l) = f(\mathbf{F}(n, m, r, l))$. Это — случайные булевы функции, некоторым образом распределённые на G_n. В § 1 мы хотим доказать,

что некоторые свойства распределения $\mathbf{f}(n, m, r)$ аналогичны свойствам равномерного распределения на G_n. Более точно, мы докажем, что при подходящем выборе n, m, r, t для любого $E \subseteq B_n$ такого, что $|E| \leqslant t$, распределение $\mathbf{f}_E(n, m, r)$ близко к равномерному на $\{0, 1\}^E$ (здесь и далее через f_E обозначается ограничение булевой функции f на множество $E \subseteq B_n$).

Предварительно докажем одну вспомогательную лемму. Пусть V — линейное пространство над полем $\mathbf{F}_2$ размерности d; $\mathbf{v}$ — некоторый случайный вектор, каким-то образом распределённый на V, а $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r$ — его независимые копии. Положим

$$\mathbf{v}^{(r)} \rightleftharpoons \bigoplus_{i=1}^{r} \mathbf{v}_i.$$

Тогда из общей теории марковских цепей вытекает, что если $\mathbf{P}[\mathbf{v}=0]>0$ и $\mathbf{v}$ не сосредоточен ни в каком собственном линейном подпространстве пространства V, то при $r \to \infty$ распределение $\mathbf{v}^{(r)}$ стремится к равномерному. Следующая ниже лемма оценивает скорость сходимости. Автор глубоко благодарен Б. А. Севастьянову, указавшему на возможность существенного упрощения доказательства этой леммы.

ЛЕММА 1. *Пусть* $\{v_1, \ldots, v_d\}$ *— базис в* V; $p = \min\{\mathbf{P}[\mathbf{v}=0], \mathbf{P}[\mathbf{v}=v_1], \ldots, \mathbf{P}[\mathbf{v}=v_d]\}$. *Тогда для любого* $v \in V$ *справедлива оценка*

$$|\mathbf{P}[\mathbf{v}^{(r)}=v] - 2^{-d}| \leqslant e^{-2pr}.$$

Доказательство. Обозначим через $\langle\ \rangle$ скалярное произведение на V, заданное формулой $\langle v_i, v_j\rangle = \delta_{ij}$ (δ_{ij} — символ Кронекера). Обозначим $\mathbf{P}[\mathbf{v}=v]$ через p_v и положим

$$\Delta_v \rightleftharpoons \sum_{w \in V} p_w (-1)^{\langle w, v\rangle}. \tag{5}$$

Тогда

$$\sum_{v \in V} \Delta_v (-1)^{\langle u, v\rangle} = \sum_{v \in V} \sum_{w \in V} p_w (-1)^{\langle u \oplus w, v\rangle} =$$

$$= \sum_{w \in V} p_w \sum_{v \in V} (-1)^{\langle u \oplus w, v\rangle} = 2^d p_u,$$

так как

$$\sum_{v \in V} (-1)^{\langle x, v\rangle} = \begin{cases} 0, & \text{если } x \neq 0 \\ 2^d, & \text{если } x = 0. \end{cases}$$

Итак,

$$p_u = 2^{-d} \sum_{v \in V} \Delta_v (-1)^{\langle u, v\rangle} \tag{6}$$

Пусть теперь даны два случайных независимых вектора $\mathbf{v}_1$ и $\mathbf{v}_2$ с распределениями $\mathbf{P}[\mathbf{v}_i=u]=2^{-d}\sum\limits_{v\in V}\Delta_v^{(i)}(-1)^{\langle u,\,v\rangle}(i=1,2)$.

Тогда

$$\mathbf{P}[\mathbf{v}_1\oplus\mathbf{v}_2=u]=\sum_{u_1\in V}\mathbf{P}[\mathbf{v}_1=u_1]\cdot\mathbf{P}[\mathbf{v}_2=u\oplus u_1]=$$

$$=2^{-2d}\sum_{u_1}\sum_{v_1}\sum_{v_2}\Delta_{v_1}^{(1)}\Delta_{v_2}^{(2)}(-1)^{(\langle u_1,\,v_1\rangle\,\oplus\,\langle u\oplus u_1,\,v_2\rangle)}=$$

$$2^{-2d}\sum_{v_1}\sum_{v_2}\Delta_{v_1}^{(1)}\Delta_{v_2}^{(2)}(-1)^{\langle u,\,v_2\rangle}\sum_{u_1}(-1)^{\langle u_1,\,v_1\oplus v_2\rangle}=$$

$$=2^{-d}\sum_{v}\Delta_v^{(1)}\Delta_v^{(2)}(-1)^{\langle u,\,v\rangle}.$$

Отсюда и из (6) получаем

$$\mathbf{P}[\mathbf{v}^{(r)}=u]=2^{-d}\sum_{v\in V}\Delta_v{}^r(-1)^{\langle u,\,v\rangle}. \tag{7}$$

Далее, $\Delta_0=1$ согласно (5). Если же $v\neq 0$, то существуют $w_1, w_2\in\{0, v_1, \ldots, v_d\}$, для которых $\langle w_1, v\rangle\neq\langle w_2, v\rangle$ и, следовательно, $|\Delta_v|\leqslant 1-2p$. Поэтому из (7) вытекает

$$|\mathbf{P}[\mathbf{v}^{(r)}=u]-2^{-d}|\leqslant\max_{\substack{v\in V\\ v\neq 0}}|\Delta_v{}^r|\leqslant(1-2p)^r\leqslant e^{-2pr}.$$

Лемма 1 доказана.

Напомним, что $\mathbf{f}(n, m, r)=f(\mathbf{F}(n, m, r))$, где случайная формула $\mathbf{F}(n, m, r)$ задаётся с помощью (3), а f_E обозначает ограничение булевой функции f на E.

ЛЕММА 2. *Пусть m, r, d — натуральные числа; $d\leqslant 2^{m-1}$ и даны $E\subseteq B_n$; $|E|=d$ и $\varphi\in\{0, 1\}^E$. Тогда*

$$|\mathbf{P}[\mathbf{f}_E(n, m, r)=\varphi]-2^{-d}|\leqslant e^{-(r/2^m)}. \tag{8}$$

Доказательство. Определим случайные булевы функции $\mathbf{f}(n, m)$ и $\mathbf{f}(n)$ соотношениями, аналогичными (3) и (4):

$$\mathbf{f}(n, m)\rightleftharpoons\mathop{\&}_{\beta=1}^{m}\bigoplus_{\gamma=1}^{n}(\lambda_{\beta\gamma}x_\gamma\oplus\lambda_\beta);$$

$$\mathbf{f}(n)\rightleftharpoons\bigoplus_{\gamma=1}^{n}(\lambda_\gamma x_\gamma\oplus\lambda),$$

где все λ независимы и равномерно распределены на $\{0, 1\}$. Заметим, что $\mathbf{f}(n, m, r)$ является суммой по mod 2 r независимых экземпляров $\mathbf{f}(n, m)$. Мы собираемся применить лемму 1 в ситуации $V=\{0, 1\}^E$; $\mathbf{v}=\mathbf{f}_E(n, m)$.

В качестве базиса $\{v_1, \ldots, v_d\}$ возьмём функции $\{\chi_\varepsilon | \varepsilon \in E\}$, где $\chi_\varepsilon(\delta) = 1 \Leftrightarrow \delta(\delta \in E;\ \chi_\varepsilon \in \{0,1\}^E)$. Очевидно, для любого $\varepsilon \in B_n$ имеем $\mathbf{P}[\mathbf{f}(n)(\varepsilon) = 1] = 1/2$. Более того, если $\varepsilon_1 \neq \varepsilon_2$, то $\mathbf{f}(n)(\varepsilon_1)$ и $\mathbf{f}(n)(\varepsilon_2)$ — две различные ненулевые линейные формы от случайных независимых величин $\{\lambda_\tau, \lambda\}$, равномерно распределённых на $\{0, 1\}$. Поэтому $\mathbf{f}(n)(\varepsilon_1)$ и $\mathbf{f}(n)(\varepsilon_2)$ независимы и, в частности,

$$\mathbf{P}[\mathbf{f}(n)(\varepsilon_1) = 1 | \mathbf{f}(n)(\varepsilon_2) = 1] = 1/2 (\varepsilon_1 \neq \varepsilon_2). \tag{9}$$

Так как $\mathbf{f}(n, m)$ — коньюнкция m независимых экземпляров $\mathbf{f}(n)$, то из (9) вытекает

$$\left.\begin{array}{l} \mathbf{P}[\mathbf{f}(n, m)(\varepsilon_1) = 1 | \mathbf{f}(n, m)\ (\varepsilon_2) = 1] = \\ = \mathbf{P}[\mathbf{f}(n, m)(\varepsilon_1) = 1] = 2^{-m} (\varepsilon_1 \neq \varepsilon_2). \end{array}\right\} \tag{10}$$

Из (10) и $d \leqslant 2^{m-1}$ получим

$$\mathbf{P}[\mathbf{f}_E(n, m) = 0] = \mathbf{P}[\forall \varepsilon \in E \mathbf{f}(n, m)(\varepsilon) = 0] \geqslant$$

$$\geqslant 1 - |E| \cdot 2^{-m} \geqslant \frac{1}{2};$$

$$\mathbf{P}[\mathbf{f}_E(n, m) = \chi_\varepsilon] = \mathbf{P}[\mathbf{f}(n, m)(\varepsilon) = 1 \,\&\, \forall \delta \in E\ (\delta \neq \varepsilon \Rightarrow$$

$$\Rightarrow \mathbf{f}(n, m)\ (\delta) = 0)] = \mathbf{P}[\mathbf{f}(n, m)(\varepsilon) = 1]\, \mathbf{P}[\forall \delta \in E\ (\delta \neq \varepsilon \Rightarrow$$

$$\Rightarrow \mathbf{f}(n, m)\ (\delta) = 0) | \mathbf{f}(n, m)(\varepsilon) = 1] \geqslant$$

$$\geqslant 2^{-m} \left(1 - \sum_{\substack{\delta \in E \\ \delta \neq \varepsilon}} \mathbf{P}[\mathbf{f}(n, m)(\delta) = 1 | \mathbf{f}(n, m)\ (\varepsilon) = 1]\right) \geqslant$$

$$\geqslant 2^{-m}(1 - d \cdot 2^{-m}) \geqslant 2^{-m-1}.$$

Таким образом, $\min\{\mathbf{P}[\mathbf{f}_E = 0],\ \mathbf{P}[\mathbf{f}_E = \chi_\varepsilon]\ (\varepsilon \in E)\} \geqslant 2^{-m-1}$. Доказательство завершается применением леммы 1.

Лемма 2 сама по себе не позволяет сделать никакого вывода о строении случайной функции $\mathbf{f}_E(n, m, r)$ в случае, когда $|E|$ велико по сравнению с r. Иногда это становится возможным, если дополнительно использовать следующую лемму:

Лемма 3. *Пусть $t \geqslant 2s$ — натуральные числа; $0 < \Theta$, $\delta < 1$; $A_1, A_2, \ldots, A_t$ — события такие, что*

$$\forall I \subseteq \{1, \ldots, t\} (|I| \leqslant s \Rightarrow |\mathbf{P}[\underset{i \in I}{\&} A_i] - \Theta^{|I|}| \leqslant \delta). \tag{11}$$

Тогда

$$\mathbf{P}\left[\bigvee_{i=1}^{t} A_i\right] \geqslant 1 - e^{-\Theta t} - \binom{t}{s+1} (\delta s + \Theta^s).$$

Доказательство. Рассмотрим вначале случай, когда s четно. Введем в рассмотрение независимые события $B_1, B_2, \ldots, B_t$, каждое из которых имеет вероятность Θ. Запишем вероятности

$\mathbf{P}\left[\bigvee_{i=1}^{t} A_i\right]$ и $\mathbf{P}\left[\bigvee_{i=1}^{t} B_i\right]$ по формуле включений и исключений:

$$\left.\begin{aligned}\mathbf{P}\left[\bigvee_{i=1}^{t} A_i\right] &= \sum_{\nu=1}^{t}(-1)^{\nu+1}\sum_{|I|=\nu}\mathbf{P}\left[\&_{i\in I} A_i\right] \geqslant \\ \geqslant \sum_{\nu=1}^{s}(-1)^{\nu+1}&\sum_{|I|=\nu}\mathbf{P}\left[\&_{i\in I} A_i\right]\end{aligned}\right\} \tag{12}$$

(неравенство верно при четном s);

$$\left.\begin{aligned}\mathbf{P}\left[\bigvee_{i=1}^{t} B_i\right] &= \sum_{\nu=1}^{t}(-1)^{\nu+1}\sum_{|I|=\nu}\Theta^{|I|} \leqslant \\ \leqslant \sum_{\nu=1}^{s}(-1)^{\nu+1}&\sum_{|I|=\nu}\Theta^{|I|} + \sum_{|I|=s+1}\Theta^{s+1}.\end{aligned}\right\} \tag{13}$$

С другой стороны, из (11) вытекает оценка

$$\sum_{\nu=1}^{s}(-1)^{\nu+1}\sum_{|I|=\nu}\mathbf{P}\left[\&_{i\in I} A_i\right] > \sum_{\nu=1}^{s}(-1)^{\nu+1}\sum_{|I|=\nu}\Theta^{|I|} - \delta s\binom{t}{s}. \tag{14}$$

Кроме того, в силу независимости B_i,

$$\mathbf{P}\left[\bigvee_{i=1}^{t} B_i\right] = 1-(1-\Theta)^t > 1-e^{-\Theta t}. \tag{15}$$

Из (12), (14), (13), (15) для четного s вытекает

$$\mathbf{P}\left[\bigvee_{i=1}^{t} A_i\right] > 1-e^{-\Theta t}-\delta s\binom{t}{s}-\Theta^{s+1}\binom{t\rightarrow}{s+1} >$$

$$> 1-e^{-\Theta t}-\binom{t\rightarrow}{s+1}(\delta s+\Theta^{s+1}).$$

Если же s нечётно, то достаточно в выше приведённых рассуждениях изменить значение s на $(s-1)$. Лемма доказана.

§ 2. СЛОЖНОСТЬ КОМБИНАТОРНЫХ ЗАДАЧ

Комбинаторные объекты, которые мы будем рассматривать, суть неориентированные графы (без петель и кратных рёбер), турниры и двудольные графы. Зафиксируем способ кодировки этих объектов булевыми функциями.

Через $\leqslant$ обозначим произвольный (например, лексикографический) линейный порядок на B_n. Булева функция $f(x_1, \ldots, x_n, \ldots, x_{2n})$ кодирует неориентированный граф $G(f)$ с множеством вершин B_n; турнир $T(f)$ с тем же множеством вершин и двудольный граф $H(f) \subseteq B_n \times B_n$ следующим обра-

зом:

$$G(f) \rightleftharpoons \langle B_n; \{(\varepsilon, \delta) \mid \varepsilon, \delta \in B_n \& \varepsilon < \delta \& f(\varepsilon, \delta) = 1\} \rangle;$$

$$T(f) \rightleftharpoons \langle B_n; \{\langle \varepsilon, \delta \rangle \mid (\varepsilon < \delta \& f(\varepsilon, \delta) = 1) \vee$$

$$\vee (\delta < \varepsilon \& f(\delta, \varepsilon) = 0)\} \rangle;$$

$$H(f) \rightleftharpoons \{\langle \varepsilon, \delta \rangle \mid f(\varepsilon, \delta) = 1\}.$$

Через $L_k(f)$ будем обозначать *сложность реализации* функции f формулами глубины k в базисе $\{\&, \oplus\}$, т. е. минимальный возможный размер $s(F)$ формулы F глубины k в базисе $\{\&, \oplus\}$ такой, что $f(F) = f$.

Наш первый пример связан с теоремой Рамсея. Через $\omega(G)$ обозначается количество вершин в максимальном полном подграфе графа G. Положим $\bar{\omega}(G) \rightleftharpoons \max\{\omega(G), \omega(\text{co}-G)\}$, где $\text{co}-G$ — граф, дополнительный к графу G. Пусть граф G_n имеет 2^n вершин, тогда о пределах, в которых может изменяться значение $\bar{\omega}(G_n)$, известны следующие результаты:

а) неконструктивно доказано существование графов G_n с $\bar{\omega}(G_n) \leqslant 2n$ ([2], с. 24);

б) $\min\limits_{G_n} \bar{\omega}(G_n) \geqslant n$ ([2], с. 24);

в) построен явный пример графов G_n таких, что $\bar{\omega}(G_n) \leqslant 2^{n^{3/4}}$ ([4, 3]).

Теорема 1. *Существует последовательность булевых функций* $f_n(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n})$ *такая, что*

$$L_3(f_n) = O(n^5 \log n)$$

и

$$\bar{\omega}(G(f_n)) \leqslant 2n$$

для достаточно больших n.

Доказательство. Положим $m = \lfloor 2\log_2 n + 3 \rfloor$, $r = \lfloor 40n^4 \rfloor$ и рассмотрим случайную булеву функцию $\mathbf{f} = \mathbf{f}(2n, m, r)$. Тогда

$$\left.\begin{aligned} &\mathbf{P}[\bar{\omega}(G(\mathbf{f})) \geqslant 2n+1] = \mathbf{P}[\exists V \subseteq B_n (|V| = 2n+1 \& \\ &\& (K(V) \subseteq G(\mathbf{f}) \vee K(V) \cap G(\mathbf{f}) = \varnothing)], \end{aligned}\right\} \qquad (16)$$

где через $K(V)$ здесь и далее обозначается полный граф с множеством вершин V. Положим $E(V) = \{\langle \varepsilon, \delta \rangle \mid \varepsilon, \delta \in V \& \varepsilon < \delta\}$. Тогда условие $K(V) \subseteq G(\mathbf{f}) \vee K(V) \cap G(\mathbf{f}) = \varnothing$ записывается в виде $\mathbf{f}_{E(V)} = 0 \vee \mathbf{f}_{E(V)} = 1$. Если $|V| = 2n+1$, то $|E(V)| = n(2n+1)$ и выполнена посылка $d \leqslant 2^{m-1}$ леммы 2 (при $d = n(2n+1)$). Применив эту лемму, получим

$$\mathbf{P}[\mathbf{f}_{E(V)} = 1 \vee \mathbf{f}_{E(V)} = 0] = O(2^{-n(2n+1)}). \qquad (17)$$

Из (16) и (17) находим

$$P[\bar{\omega}(G(\mathbf{f})) \geqslant 2n+1] = O\left(\binom{2^n}{2n+1} \cdot 2^{-n(2n+1)}\right) = o(1)$$

и, значит, для некоторой формулы $F_n \in \mathfrak{M}(2n, m, r)$ справедливо $\bar{\omega}(G(f(F_n))) \leqslant 2n$. Кроме того, $s(F_n) \leqslant 2nmr = O(n^5 \log n)$. Теорема 1 доказана.

Наш следующий пример аналогичен только что рассмотренному. Турнир T называется *транзитивным*, если существует упорядочение σ его игроков такое, что $(i, j) \in T$ тогда и только тогда, когда $\sigma(i) < \sigma(j)$. Через $v(T)$ обозначим количество игроков в максимальном транизитивном подтурнире турнира T. Пусть множество игроков турнира T_n есть B_n. Известно, что

а) существуют турниры T_n с $v(T_n) \leqslant 2n+1$ ([2], с. 7);

б) $\min\limits_{T_n} v(T_n) \geqslant n+1$ ([2], с. 7).

Теорема 2. *Существует последовательность булевых функций* $f_n(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{2n})$ *такая что*

$$L_3(f_n) = O(n^5 \log n)$$

и

$$v(T(f_n)) \leqslant 2n+1$$

для достаточно больших n.

Доказательство проводится аналогично доказательству предыдущей теоремы. Надо лишь вместо множеств V мощности $(2n+1)$ рассмотреть множества мощности $(2n+2)$ и событие $(\mathbf{f}_{E(V)} = 1 \vee \mathbf{f}_{E(V)} = 0)$ заменить на событие «$\mathbf{f}_{E(V)}$ задает транзитивный турнир на множестве игроков V». Тогда можно доказать оценку

$$\mathbf{P}[v(T(\mathbf{f})) \geqslant 2n+2] = O\left(\binom{2^n}{2n+2}(2n+2)! \cdot 2^{-(n+1)(2n+1)}\right) =$$

$$= O(2^{n(2n+2)-(n+1)(2n+1)}) = o(1),$$

после чего доказательство теоремы 2 завершается аналогично доказательству теоремы I.

Два следующих примера относятся к формулам глубины 4. Первый из них показывает, что с помощью таких формул можно строить множества «общего положения» в линейных пространствах над F_2.

Пусть $S \subseteq B_n$ (B_n рассматривается как линейное пространство над полем F_2); x, y — вещественные числа. Скажем, что S обладает (x, y)-*свойством*, если $\forall L$ (L — линейное подпространство в $B_n \& \dim(L) \leqslant x \Rightarrow |L \cap S| < y$). Булевой функции $f(x_1, \ldots, x_n)$ ставится в соответствие множество $S(f) \subseteq B_n$, состоящее из тех $\varepsilon \in B_n$, для которых $f(\varepsilon) = 1$.

Теорема 3. *Пусть* $0<\alpha<1$; $\alpha<\beta$. *Тогда существует последовательность булевых функций* $f_n(x_1, \ldots, x_n)$ *такая, что* $L_4(f_n)=O(n^3\log n)$, $S(f_n)$ *обладает* $(\alpha n, \beta n)$*-свойством для достаточно больших* n *и*

$$|S(f_n)|=\Omega\left(2^{n\left(1-\frac{\alpha}{\beta}\right)(1-\alpha)}\right).$$

Доказательство. Пусть $m=\lfloor \log_2(3\beta n)\rfloor$, $r=\lfloor 6\beta^2 n^2\rfloor$, $l=\left\lfloor\left(\alpha+\frac{\alpha(1-\alpha)}{\beta}\right)n+\frac{4}{\beta}\right\rfloor$. Рассмотрим вначале случайную функцию $\mathbf{f}(n, m, r)$ и применим к ней лемму 2 для двух значений $d: d=1$ и $d=\lfloor \beta n\rfloor$. Мы получим:

$$\forall \varepsilon\in B_n \mathbf{P}[\mathbf{f}(n, m, r)=1]=2^{-1}(1+O(e^{-\beta n})), \tag{18}$$

$$\forall E\subseteq B_n(|E|=\lfloor \beta n\rfloor \Rightarrow \mathbf{P}[\mathbf{f}_E(n, m, r)=1]=$$

$$=2^{-\lfloor \beta n\rfloor}\left(1+O\left(\left(\frac{e}{2}\right)^{-\beta n}\right)\right). \tag{19}$$

Обозначим теперь $\mathbf{g}=\mathbf{f}(n, m, r, l)$. Так как $\mathbf{g}$ является коньюнкцией l независимых экземпляров $\mathbf{f}(n, m, r)$ и $l<n$, то из (18) и (19) соответственно вытекает

$$\forall \varepsilon\in B_n \mathbf{P}[\mathbf{g}(\varepsilon)=1]=2^{-l}(1+o(1)), \tag{20}$$

$$\forall E\subseteq B_n(|E|=\lfloor \beta n\rfloor \Rightarrow \mathbf{P}[\mathbf{g}_E=1]=2^{-\lfloor \beta n\rfloor-l}(1+o(1))). \tag{21}$$

Суммируя (20) по всем $\varepsilon\in B_n$, получим

$$\mathbf{M}[|S(\mathbf{g})|]=2^{n-l}(1+o(1)). \tag{22}$$

Введем обозначение

$T\rightleftharpoons\{E\subseteq B_n \mid |E|=\lfloor \beta n\rfloor \& E$ порождает линейное подпространство размерности $\leqslant \alpha n\}$.

Тогда, с учетом (21),

$$\left.\begin{aligned}&\mathbf{P}[S(\mathbf{g}) \text{ не обладает } (\alpha n, \beta n)\text{-свойством}]=\\&=\mathbf{P}[\exists E\in T(\mathbf{g}_E=1)]=O(|T|\cdot 2^{-\lfloor \beta n\rfloor-l}).\end{aligned}\right\} \tag{23}$$

Оценим сверху $|T|$. Каждый элемент $E\in T$ допускает разбиение $\langle E', E''\rangle$, где $E'\cup E''=E$; $E'\cap E''=\varnothing$; $|E'|=[\alpha n]$; E'' содержится в линейном пространстве, порожденном множеством E'. $|T|$ не превышает числа пар $\langle E', E''\rangle$, обладающих указанными свойствами. Компоненту E' можно выбрать не более, чем $(2^n)^{\alpha n}=2^{(\alpha n^2)}$ способами. После того, как E' выбрано, любой вектор в E'', который является линейной комбинацией векторов из E', можно выбрать не более, чем $2^{\alpha n}$ способами. Следовательно, вторую компоненту E'' (при фиксированном E') можно выбрать не более, чем $2^{\alpha n((\beta-\alpha)n+2)}$ способами. Окончательно получаем оценку $|T|\leqslant 2^{n^2(\alpha+\alpha(\beta-\alpha))+2\alpha n}$. Подставляя ее в (23), убеждаемся, что

$$\mathbf{P}[S(\mathbf{g}) \text{ не обладает } (\alpha n, \beta n)\text{-свойством}]=O(2^{-n}). \tag{24}$$

По формуле полного математического ожидания, $\mathbf{M}[|S(\mathbf{g})|] = \mathbf{M}[|S(\mathbf{g})| \mid |S(\mathbf{g})$ обладает $(\alpha n, \beta n)$-свойством$] \times \mathbf{P}[S(\mathbf{g})$ обладает $(\alpha n, \beta n)$-свойством $] + \mathbf{M}[|S(\mathbf{g})| \mid |S(\mathbf{g})$ не обладает $(\alpha n, \beta n)$-свойством$] \times \mathbf{P}[S(\mathbf{g})$ не обладает $(\alpha n, \beta n)$-свойством$]$. Подставив сюда (24) и заметив, что заведомо $|S(\mathbf{g})| \leqslant 2^n$, получим

$$\mathbf{M}[|S(\mathbf{g})|] \leqslant \mathbf{M}[|S(\mathbf{g})| \mid |S(\mathbf{g})$$ обладает $(\alpha n, \beta n)$-свойством$] + O(1).$$

Далее, с учетом (22) и соотношения $n - l \to \infty$, найдем

$$\mathbf{M}[|S(\mathbf{g})| \mid |S(\mathbf{g})$$ обладает $(\alpha n, \beta n)$-свойством$] = \Omega(2^{n-l}).$$

Следовательно, можно выбрать $F_n \in \mathfrak{M}(n, m, r, l)$ так, что $S(f(F_n))$ обладает $(\alpha n, \beta n)$-свойством и $|S(f(F_n))| = \Omega(2^{n-l})$. Кроме того, $s(F_n) \leqslant nmrl = O(n^3 \log n)$. Теорема 3 доказана.

Второй пример, относящийся к схемам глубины 4, связан с проблемой Царанкевича ([2], с. 62). Скажем, что двудольный граф $H \subseteq A_1 \times A_2$ обладает (a, b)-*свойством*, если $\forall B_1 \subseteq A_1 \forall B_2 \subseteq A_2 (|B_1| = a \,\&\, |B_2| = b \Rightarrow B_1 \times B_2 \not\subseteq H)$. Проблема Царанкевича заключается в определении максимального числа рёбер $k_{ab}(|A_1|, |A_2|)$ в двудольном графе $H \subseteq A_1 \times A_2$, обладающим (a, b)-свойством. Мы ограничимся рассмотрением случая $a = b = \text{const}$, $A_1 = A_2 = B_n$, $n \to \infty$. Относительно него известны следующие факты:

а) существуют H_n, обладающие (a, a)-свойством и такие, что $|H_n| = \Omega\left(2^{n\left(2 - \frac{2}{a}\right)}\right)$ ([2], с. 64),

б) $\max\{|H_n| \mid H_n$ обладает (a, a)-свойством$\} = O\left(2^{n\left(2 - \frac{1}{a}\right)}\right)$ ([2], с. 64).

Теорема 4. *Для любого* $a \geqslant 2$ *существует последовательность булевых функций* $f_n(x_1, \ldots, x_n, \ldots, x_{2n})$ *такая, что*
$L_4(f_n) = O(n^2 \log n)$,
$H(f_n)$ *обладает* (a,a)*-свойством и*

$$|H(f_n)| = \Omega\left(2^{n\left(2 - \frac{2a}{a^2-1}\right)}\right).$$

Доказательство. Пусть $m = \lfloor \log_2(2a^2) \rfloor$, $r = \lfloor 5a^2 \log_2 n \rfloor$, $l = \left\lfloor n \frac{2a}{a^2-1} + 1 \right\rfloor$. Вводя обозначение $\mathbf{g} = \mathbf{f}(2n, m, r, l)$ и рассуждая аналогично доказательству теоремы 3, получим

$$\forall E \subseteq B_n \times B_n (|E| = a^2 \Rightarrow \mathbf{P}[\mathbf{g}_E = 1] = 2^{-a^2 l}(1 + o(1)),$$

$$\mathbf{M}[|H(\mathbf{g})|] \geqslant \frac{1}{2} \cdot 2^{2n-l}. \tag{25}$$

Аналогично (23), получим из (25), что $\mathbf{P}[H(\mathbf{g})$ не обладает (a, a)-свойством$] = 2^{2na - a^2 l}(1 + o(1))$. Далее, $2^{2n} \cdot \mathbf{P}[\mathbf{H}(\mathbf{g})$ не обладает

(a, a)-свойством] $= 2^{2n+2na-a^2l}(1+o(1)) \leqslant \frac{1}{3} \cdot 2^{2n-l}$. После этого доказательство завершается аналогично доказательству теоремы 3.

Рассмотрим теперь несколько более сложные примеры применения нашей техники.

Говорят, что турнир T обладает *свойством* $S(k)$, если для всякого множества V из k игроков найдется какой-либо другой игрок, победивший всех игроков из V. Пусть снова B_n есть множество игроков турнира T_n. Тогда, если T_n обладает $S(k)$-свойством, то $k \leqslant n$; с другой стороны, доказано существование турниров T_n со свойством $S(n(1-o(1)))$ ([2], с. 42).

Теорема 5. *Существует последовательность булевых функций* $S_n(x_1, \ldots, x_n, \ldots, x_{2n})$ *такая, что*

$$L_3(f_n) = O(n^7 \log n)$$

и турнир $T(f_n)$ *обладает* $S(n(1-o(1)))$*-свойством.*

Доказательство. Зафиксируем следующие значения параметров: $m = [\log_2(64n^3)]$, $r = [3000n^6]$, $k = [n - 2\log_2 n]$, $s = \lfloor 20n^2 \rfloor$. Пусть $\mathbf{f} = f(2n, m, r)$, тогда

$$\left.\begin{aligned}\mathbf{P}[T(\mathbf{f}) \text{ не обладает свойством } S(k)] = \mathbf{P}[\exists V_0 \subseteq \\ \subseteq B_n (|V_0| = k \,\&\, \neg(\exists v \in B_n \setminus V_0 \forall v_0 \in V_0 \langle v, v_0 \rangle \in T(\mathbf{f})))].\end{aligned}\right\} \quad (26)$$

Обозначим для $v \notin V_0$ через $E(V_0, v)$ множество наборов из $B_n \times B_n$, от которых зависят дуги из $V_0 \times \{v\}$:

$$E(V_0, v) = \{\langle v_0, v \rangle \mid v_0 \in V_0 \,\&\, v_0 < v\} \cup \{\langle v, v_0 \rangle \mid v_0 \in V_0 \,\&\, v < v_0\}.$$

Тогда событие $\forall v_0 \in V_0 \langle v, v_0 \rangle \in T(\mathbf{f})$ записывается в виде $\mathbf{f}_{E(V_0, v)} = \varphi_{E(V_0, v)}$, где $\varphi_{E(V_0, v)}$ — некоторая функция из $\{0, 1\}^{E(V_0, v)}$. Пронумеруем элементы множества $B_n \setminus V_0$: $B_n \setminus V_0 = \{v_1, \ldots, v_t\}$ $(t = 2^n - k)$ и обозначим через A_i $(1 \leqslant i \leqslant t)$ событие $\mathbf{f}_{E(V_0, v_i)} = \varphi_{E(V_0, v_i)}$. Тогда для любого $I \subseteq \{1, \ldots, t\}$ для множества $\bigcup_{i \in I} E(V_0, v_i)$ мощности $d \leqslant ks$ можно применить лемму 2. Мы получим

$$\left|\mathbf{P}\left[\&_{i \in I} \mathbf{f}_{E(V_0, v_i)} = \varphi_{E(V_0, v_i)}\right] - 2^{-k|I|}\right| \leqslant e^{-20n^3}.$$

Далее, на основании леммы 3 $(\Theta = 2^{-k}, \delta = e^{-20n^3})$,

$$\mathbf{P}\left[\neg\left(\bigvee_{i=1}^{t} A_i\right)\right] = O\left(e^{-t/2^k} + \binom{t}{s+1}(e^{-20n^3} + 2^{-ks})\right) = O(2^{-n^3}).$$

Учитывая (26), найдем

$$\mathbf{P}[T(\mathbf{f}) \text{ не обладает свойством } S(k)] = O\left(\binom{2^n}{k} \cdot 2^{(-n^3)}\right) = o(1).$$

Следовательно, найдется формула $F_n \in \mathfrak{M}(2n, m, r)$ такая, что $T(f(F_n))$ обладает свойством $S(k)$ и $s(F_n) \leqslant 2nmr = O(n^7 \log n)$. Теорема доказана.

Два наших последних примера относятся к ассиметрическим графам ([2, с. 82—88]). *Ассиметрия* $A(G)$ неориентированного графа G определяется соотношением $A(G) \rightleftharpoons \min\{|D| \mid G \triangle D$ обладает нетривиальным автоморфизмом$\}$ (D — некоторое множество дуг).

Максимальная возможная ассиметрия $A(G_n)$ графа G_n с 2^n вершинами равна $2^n\left(\frac{1}{2} - o(1)\right)$ ([2]).

Теорема 6. *Пусть* $0 < \varepsilon < \frac{1}{12}$. *Тогда существует последовательность булевых функций* $f_n(x_1, \ldots, x_{2n})$ *такая, что* $L_3(f_n) = O(n^{17-8\log_2 \varepsilon} \log n)$; $L_5(f_n) = O(n^5 \log n)$ *и*

$$A(G(f_n)) \geqslant \left(\frac{1}{12} - \varepsilon\right) \cdot 2^n$$

для достаточно больших n.

Доказательство. Рассмотрим следующий граф:

$$G_0 \rightleftharpoons G\left(\bigoplus_{i=1}^{n} x_i x_{n+i}\right). \tag{27}$$

Если обозначить через $\langle\ \rangle$ скалярное произведение на B_n, задаваемое формулой $\langle (\varepsilon_1, \ldots, \varepsilon_n), (\delta_1, \ldots, \delta_n) \rangle = \bigoplus_{i=1}^{n} \varepsilon_i \delta_i$, то

$$G_0 = \langle B_n,\ \{(\varepsilon, \delta) \mid \langle \varepsilon, \delta \rangle = 1\} \rangle .$$

Напомним, что $S(f(x_1, \ldots, x_n)) = \{\varepsilon \in B_n \mid f(\varepsilon) = 1\}$ и $K(V) = \{(\varepsilon, \delta) \mid \varepsilon \neq \delta \& \varepsilon,\ \delta \in V\}$ для $V \subseteq B_n$. Заметим, что

$$K(S(f)) = G(f(x_1, \ldots, x_n) \& f(x_{n+1}, \ldots, x_{2n})).$$

Фиксируем теперь следующие значения параметров: $m = \left\lfloor \log_2\left(\frac{32n^2}{\varepsilon}\right) \right\rfloor$, $r = \left\lfloor \frac{1000n^4}{\varepsilon^2} \right\rfloor$, $l = \left\lfloor \log_2\left(\frac{2}{\varepsilon}\right) \right\rfloor$, $d = \left\lfloor \frac{8n^2}{\varepsilon} \right\rfloor$. Введем в рассмотрение случайные булевы функции $\mathbf{f} = \mathbf{f}(n, m, r)$ и $\mathbf{g} = \mathbf{f}(n, m, r, l)$ и определим случайный граф $\mathbf{G}$ формулой

$$\mathbf{G} = G_0 \triangle K(S(\mathbf{g})). \tag{29}$$

Тогда

$$\left.\begin{aligned} &\mathbf{P}\left[A(\mathbf{G}) \leqslant \left(\frac{1}{12} - \varepsilon\right) \cdot 2^n\right] = \mathbf{P}\,[\exists \sigma - \text{неединичная перестановка множества } B_n \exists D \subseteq K(B_n) \left(|D| \leqslant \left(\frac{1}{12} - \varepsilon\right) 2^n \,\&\right. \\ &\left.\& \sigma(\mathbf{G}) \triangle \mathbf{G} = \sigma(D) \triangle D)] \leqslant \mathbf{P}\left[\exists \sigma - \text{неединичная перестановка множества } B_n \left(|\sigma(\mathbf{G}) \triangle \mathbf{G}| \leqslant \left(\frac{1}{12} - \varepsilon\right) 2^{n+1}\right)\right]. \end{aligned}\right\} \tag{30}$$

Пусть теперь

$$\left.\begin{aligned} &\mathrm{Aut} \rightleftharpoons \{\sigma \mid \sigma(G_0) = G_0\} = \\ &= \{\sigma \mid \forall \varepsilon,\ \delta \in B_n (\langle \varepsilon,\ \delta \rangle = \langle \sigma(\varepsilon), \sigma(\delta) \rangle)\} \end{aligned}\right\} \tag{31}$$

Установим три простых свойства множества Aut.

Утверждение 1°. $\sigma\in\mathrm{Aut}\Rightarrow\sigma$ — *линейный автоморфизм.*

В самом деле, для всех $u, v, x\in B_n$ имеем

$\langle\sigma(u)\oplus\sigma(v)\oplus\sigma(u\oplus v), x\rangle=\langle\sigma(u), x\rangle\oplus\langle\sigma(v), x\rangle\oplus$

$\oplus\langle\sigma(u\oplus v), x\rangle=\langle u, \sigma^{-1}(x)\rangle\oplus\langle v, \sigma^{-1}(x)\rangle\oplus$

$\oplus\langle u\oplus v, \sigma^{-1}(x)\rangle=0$. Следовательно, $\sigma(u)\oplus\sigma(v)\oplus$

$\oplus\sigma(u\oplus v)=0$.

Утверждение 2°. $|\mathrm{Aut}|\leqslant 2^{n^2}$.

Непосредственно вытекает из 1°.

Утверждение 3°. $\sigma\notin\mathrm{Aut}\Rightarrow\exists u\in B_n\left(\deg_{\sigma(G_*)\triangle G_*}(u)\geqslant\frac{1}{6}\cdot 2^n\right)$.

Рассмотрим вначале случай, когда σ линеен. Тогда $\exists u, v\in B_n$ ($\langle u, v\rangle\neq\langle\sigma(u), \sigma(v)\rangle$) и, следовательно, множество $\{x\,|\,\langle u, x\rangle=\langle\sigma(u), \sigma(x)\rangle\}$, являясь собственным линейным подпространством в B_n, имеет мощность, не превосходящую 2^{n-1}, и мы получаем $\deg_{\sigma(G_*)\triangle G_*}(\sigma(u))\geqslant 2^{n-1}$.

Если же σ не является линейным, то для некоторых $u, v\in B_n$ имеем $\sigma(u)\oplus\sigma(v)\neq\sigma(u\oplus v)$ и, следовательно, $|H|=2^{n-1}$, где $H=\{x\,|\,\langle\sigma(u), x\rangle\oplus\langle\sigma(v), x\rangle\neq\langle\sigma(u\oplus v), x\rangle\}$. Кроме того, для любого $x\in H$ имеет место хотя бы одно из трех неравенств $\langle u, \sigma^{-1}(x)\rangle\neq\langle\sigma(u), x\rangle$; $\langle v, \sigma^{-1}(x)\rangle\neq\langle\sigma(v), x\rangle$; $\langle u\oplus v, \sigma^{-1}(x)\rangle\neq\neq\langle\sigma(u\oplus v), x\rangle$, так как, разумеется, $\langle u, \sigma^{-1}(x)\rangle\oplus\langle v, \sigma^{-1}(x)\rangle=\langle u\oplus v, \sigma^{-1}(x)\rangle$. Следовательно, доказываемое утверждение справедливо хотя бы для одной из трех вершин $\sigma(u)$, $\sigma(v)$, $\sigma(u\oplus v)$.

Обратимся теперь к оценке вероятности (30). Разберем вначале случай $\sigma\in\mathrm{Aut}$; $\sigma\neq 1$. Из определений (31), (29), вытекает, что $\sigma(\mathbf{G})\triangle\mathbf{G}=\sigma(K(S(\mathbf{G})))\triangle K(S(\mathbf{G}))$ и, следовательно,

$$\left.\begin{aligned}&\mathbf{P}\left[|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant\left(\frac{1}{12}-\varepsilon\right)2^{n+1}\right]\leqslant\\&\leqslant\mathbf{P}\left[|\sigma(S(\mathbf{g}))\triangle S(\mathbf{g})|\leqslant 2^{n/2+1}\right]\quad(\sigma\in\mathrm{Aut}).\end{aligned}\right\}\tag{32}$$

Так как в силу 1° σ линеен и $\sigma\neq 1$, то $\mathrm{Ker}(1\oplus\sigma)$ — собственное линейное подпространство в B_n и, значит,

$$|\{u\,|\,\sigma(u)\neq u\}|\geqslant 2^{n-1}.\tag{33}$$

Выберем максимальную по мощности систему $\{v_1, w_1, \ldots, v_t, w_t\}$ из $2t$ попарно различных элементов B_n таких, что $\sigma(v_i)=\sigma(w_i)$. Из максимальности этой системы и (33) вытекает, что $t\geqslant 2^{n-3}$. Выделим теперь в найденной системе $\left[\frac{2^{n-3}}{d}\right]$ попарно непересекающихся подмножеств пар (v_j, w_j) по d пар в каждом:

$$V_i=\{v_1^{(i)}, w_1^{(i)}, \ldots, v_d^{(i)}, w_d^{(i)}\}\left(1\leqslant i\leqslant\left[\frac{2^{n-3}}{d}\right]\right).$$

Тогда

$$\left.\begin{aligned}&\mathbf{P}\left[|\sigma(S(\mathbf{g}))\triangle S(\mathbf{g})|<\left[\frac{2^{n-3}}{d}\right]\right]\leqslant\mathbf{P}\left[\exists 1\leqslant i\leqslant\left[\frac{2^{n-3}}{d}\right]\forall\right.\\&\left.\forall 1\leqslant j\leqslant d\,(w_j^{(i)}\in S(\mathbf{g})\Rightarrow v_j^{(i)}\in S(\mathbf{g}))\right]=\\&=O\left(2^n\cdot P\left[\forall 1\leqslant j\leqslant d\,(\mathbf{g}(w_j)=1\Rightarrow\mathbf{g}(v_j)=1)\right]\right),\end{aligned}\right\}\tag{34}$$

где $v_1, w_1, \ldots, v_d, w_d$ попарно различны. Применив к множеству $E=\{v_1, w_1, \ldots, v_d, w_d\}$ лемму 2, получим, что для любого $\varphi\in\{0,1\}^E$ справедливо

$$\mathbf{P}[\mathbf{f}_E=\varphi]=2^{-2d}(1+O(2^{2d}e^{-r/2^m})).\tag{35}$$

Рассмотрим еще случайную функцию $\hat{\mathbf{f}}_E$, равномерно распределенную на $\{0,1\}^E$. Обозначим через $\mathbf{f}_E^1, \mathbf{f}_E^2, \ldots, \mathbf{f}_E^l$ независимые экземпляры $\mathbf{f}_E$ $\left(\text{в этих обозначениях } \mathbf{g}=\underset{i=1}{\overset{l}{\&}}\mathbf{f}_E^i\right)$: а через $\hat{\mathbf{f}}_E^1, \hat{\mathbf{f}}_E^2, \ldots, \hat{\mathbf{f}}_E^l$ — независимые экземпляры $\hat{\mathbf{f}}_E$. Тогда (35) переписывается в виде

$$\mathbf{P}[\mathbf{f}_E=\varphi]=\mathbf{P}[\hat{\mathbf{f}}_E=\varphi](1+O(2^{2d}e^{-r/2^m})).\tag{36}$$

Подставляя вместо r, m, d, l их значения, убеждаемся, что

$$l2^{2d}e^{-r/2^m}=O(1).\tag{37}$$

Следовательно, для $\varphi_1, \varphi_2, \ldots, \varphi_l\in\{0,1\}^E$ из (36) вытекает

$$\mathbf{P}\left[\underset{i=1}{\overset{l}{\&}}\mathbf{f}_l^i=\varphi_i\right]=O\left(\mathbf{P}\left[\underset{i=1}{\overset{l}{\&}}\hat{\mathbf{f}}_E^i=\varphi_i\right]\right),$$

откуда получаем, что для любого события A, зависящего от $\varphi\in\{0,1\}^E$, справедлива оценка

$$\mathbf{P}[A(\mathbf{g}_E)]=O(\mathbf{P}[A(\hat{\mathbf{g}}_E)]),$$

где $\hat{\mathbf{g}}_E=\underset{i=1}{\overset{l}{\&}}\hat{\mathbf{f}}_E^i$ — случайная функция из $\{0,1\}^E$, независимо с вероятностью 2^{-l} обращающаяся в единицу на всяком входе из E. В частности,

$$\begin{aligned}&\mathbf{P}[\forall 1\leqslant j\leqslant d\,(\mathbf{g}(w_j)=1\Rightarrow\mathbf{g}(v_j)=1)]=\\&=O(\mathbf{P}[\forall 1\leqslant j\leqslant d\,(\hat{\mathbf{g}}(w_j)=1\Rightarrow\hat{\mathbf{g}}(v_j)=1)])=\\&=O((1-2^{-l}(1-2^{-l}))^d)=O(e^{-d/2^{l+1}}).\end{aligned}$$

Подставив найденную оценку в (34) и воспользовавшись свойством 2^0 множества Aut, получим

$$\left.\begin{aligned}&\mathbf{P}\left[\exists\sigma\in\mathrm{Aut}\left(\sigma\neq 1\,\&\,|\sigma(S(\mathbf{g}))\triangle S(\mathbf{g})|<\left[\frac{2^{n-3}}{d}\right]\right)\right]=\\&=O(2^{(n^2+n)}\cdot e^{-d/2^{l+1}})=o(1).\end{aligned}\right\}\tag{38}$$

Наконец, из (32) и (38) следует

$$\mathbf{P}\left[\exists\sigma\in\mathrm{Aut}\left(\sigma\neq 1\,\&\,|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant\left(\frac{1}{12}-\varepsilon\right)2^{n+1}\right)\right]=o(1). \tag{39}$$

Обратимся теперь к перестановкам $\sigma\notin\mathrm{Aut}$. Пусть σ — такая перестановка; выберем на основании 3^0 вершину u, для которой $\deg_{\sigma(G_0)\triangle G_0}(u)\geqslant\frac{1}{6}\cdot 2^n$. Если $|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant\left(\frac{1}{12}-\varepsilon\right)2^{n+1}$, то $\deg_{\sigma(\mathbf{G})\triangle\mathbf{G}}(u)\leqslant\left(\frac{1}{6}-2\varepsilon\right)2^n$ и, в силу (29), $\deg_{K(S(\mathbf{g}))\triangle\sigma(K(S(\mathbf{g})))}(u)\geqslant\geqslant\varepsilon\cdot 2^{n+1}$. Отсюда вытекает $|S(\mathbf{g})|\geqslant\varepsilon\cdot 2^n$. Следовательно,

$$\mathbf{P}\left[\exists\sigma\notin\mathrm{Aut}\left(|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant\left(\frac{1}{12}-\varepsilon\right)\cdot 2^{n+1}\right)\right]\leqslant$$

$$\leqslant\mathbf{P}[|S(\mathbf{g})|\geqslant\varepsilon\cdot 2^n]\leqslant\frac{1}{\varepsilon\cdot 2^n}\mathbf{M}[|S(\mathbf{g})|].$$

Аналогично (22) докажем, что $\mathbf{M}[|S(\mathbf{g})|]=2^{n-l+o(1)}$. Окончательно получим

$$\mathbf{P}\left[\exists\sigma\notin\mathrm{Aut}\left(|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant\left(\frac{1}{12}-\varepsilon\right)\cdot 2^{n+1}\right)\right]\leqslant 2^{o(1)-1}. \tag{40}$$

Теперь из (30), (39), (40) вытекает, что $\mathbf{P}\left[A(\mathbf{G})\geqslant\left(\frac{1}{12}-\varepsilon\right)\times\right.$ $\left.\times 2^n\right]>0$. Следовательно, в силу (29), (27), (28) найдется функция f_n вида

$$f_n=f\left(\bigoplus_{i=1}^{n}x_ix_{n+i}\oplus(F_n(x_1,\ldots,x_n)\,\&\,F_n(x_{n+1},\ldots,x_{2n}))\right), \tag{41}$$

где $F_n\in\mathfrak{M}(n,m,r,l)$, для которой $A(G(f_n))\geqslant\left(\frac{1}{12}-\varepsilon\right)\cdot 2^n$. Так как F_n — формула размера $O(n^5\log n)$ глубины 4, то оценка $L_5(f_n)=O(n^5\log n)$ вытекает из (41) непосредственно. Формулу $F_n(x_1,\ldots,x_n)\&F_n(x_{n+1},\ldots,x_{2n})\in\mathfrak{M}(n,m,r,2l)$ можно перестроить в формулу из $\mathfrak{M}(n,m,r^{2l})$ раскрыв внешние скобки. Тем самым доказано последнее утверждение теоремы:

$L_3(f_n)=O(n^{17-8\log_2\varepsilon}\log n)$.

Мера асимметрии $A'(G)$ графа G определяется аналогично $A(G)$ с одним дополнительным ограничением на перестановку σ. Это ограничение состоит в том, что σ не должна иметь неподвижных точек. $A'(G)$ является более «глобальной» характеристикой графа G, чем $A(G)$ и это подтверждается фактом, что максимальное возможное значение величины $A'(G_n)$ для графов G_n с 2^n вершинами равно $2^{2^n}\left(\frac{1}{6}+o(1)\right)$ ([2], с. 88).

Теорема 7. *Существует последовательность булевых функций* $f_n(x_1,\ldots,x_n,x_{n+1},\ldots,x_{2n})$ *такая, что*

$L_5(f_n)=O(n^7\log^2 n)$,

$A'(G(f_n))=\Omega(n^{-6}2^{2n})$.

Доказательство. Положим

$$\left.\begin{aligned} &m=\lfloor 7+3\log_2 n\rfloor,\quad r=\lfloor 2^{15}n^6\rfloor,\quad l=\lfloor 4+\log_2 n\rfloor,\\ &d=\lfloor 2^6 n^3\rfloor,\quad h=\left\lfloor\frac{2^{n-11}}{n^3}\right\rfloor. \end{aligned}\right\} \tag{42}$$

Пусть $\mathbf{f}=\mathbf{f}(n, m, r)$; $\mathbf{g}=\mathbf{f}(n, m, r, l)$. Введем те же обозначения (27), (29), (31) для G_0, $\mathbf{G}$, Aut, что и в доказательстве предыдущей теоремы. Далее, пусть $\rho(\sigma, \sigma')=|\{v|\sigma(v)\neq\sigma'(v)\}|$ — метрика Хэмминга на множестве всех перестановок и

$$\mathrm{Aut}^*=\{\sigma|\exists\sigma'\in\mathrm{Aut}(\rho(\sigma, \sigma')\leqslant h)\}.$$

Прежде всего отметим, что

$$\left.\begin{aligned} &\mathbf{P}[A'(\mathbf{G})\leqslant n^{-6}2^{2n-26}]\leqslant\mathbf{P}[\exists\sigma-\text{перестановка } B_n\\ &\forall v(\sigma(v)\neq v)\,\&\,|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant n^{-6}2^{2n-25}]. \end{aligned}\right\} \tag{43}$$

Начнем со случая $\sigma\in\mathrm{Aut}^*$; $\forall v(\sigma(v)\neq v)$. Выберем $\sigma'\in\mathrm{Aut}$ так, что $\rho(\sigma, \sigma')\leqslant h$. Из $\forall v(\sigma(v)\neq v)$ вытекает $\sigma'\neq 1$. Так как $\sigma'\in\mathrm{Aut}$, то $\sigma(\mathbf{G})\triangle\mathbf{G}=(\sigma(\mathbf{G})\triangle\sigma'(\mathbf{G}))\triangle(\sigma'(K(S(\mathbf{g})))\triangle K(S(\mathbf{g})))$. Обозначим $\sigma'(S(\mathbf{g}))\setminus S(\mathbf{g})$ через $\mathbf{S}_1$ и $\{v|\sigma^{-1}(v)\neq\sigma'^{-1}(v)\}$ через S_2. Тогда $|S_2|\leqslant h$ и $K(\mathbf{S}_1\setminus S_2)\subseteq\sigma(\mathbf{G})\triangle\mathbf{G}$.

Предположив, что $|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant n^{-6}2^{2n-25}$, получим отсюда $|\mathbf{S}_1\setminus S_2|\leqslant 3n^{-3}2^{n-13}$. Далее, $|\mathbf{S}_1|\leqslant|S_2|+|\mathbf{S}_1\setminus S_2|\leqslant h+3n^{-3}\times\times 2^{n-13}\leqslant n^{-3}2^{n-11}$. Аналогично доказывается неравенство $|S(\mathbf{g})\setminus\setminus\sigma'(S(\mathbf{g}))|\leqslant n^{-3}2^{n-11}$. Таким образом, $|\sigma'(S(\mathbf{g}))\triangle S(\mathbf{g})|\leqslant\leqslant n^{-3}2^{n-10}$. Итак, мы доказали оценку

$$\left.\begin{aligned} &\mathbf{P}[\exists\sigma\in\mathrm{Aut}^*(\forall v(\sigma(v)\neq v)\,\&\,|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant n^{-6}2^{2n-25})]\leqslant\\ &\mathbf{P}[\exists\sigma'\in\mathrm{Aut}(\sigma'\neq 1\,\&\,|\sigma'(S(\mathbf{g}))\triangle S(\mathbf{g})|\leqslant n^{-3}2^{n-10})], \end{aligned}\right\} \tag{44}$$

так как событие в левой части неравенства логически влечет событие, стоящее в правой части.

Теперь мы хотим воспользоваться оценкой (38) из доказательства теоремы 6. Для этого достаточно заметить, что соотношения, связывающие параметры n, m, r, d, l, которые были использованы при выводе (38), суть $d\leqslant 2^{m-1}$, (37) и неравенство $2^{n^2+n}e^{-d/2^{l+1}}=o(1)$ в (38); все эти соотношения истинны также для значений параметров (42). Итак, для рассматриваемого сейчас случая истинно (38).

(44) и (38) немедленно влекут оценку

$$\left.\begin{aligned} &\mathbf{P}[\exists\sigma\in\mathrm{Aut}^*(\forall v(\sigma(v)\neq v)\,\&\,|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant\\ &\leqslant n^{-6}2^{2n-25})]=o(1). \end{aligned}\right\} \tag{45}$$

Перейдем теперь к рассмотрению случая $\sigma\notin\mathrm{Aut}^*$. Снова предположим $|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant n^{-6}2^{2n-25}$. Введем обозначения

$$\left.\begin{aligned} &\mathbf{V}_+=\left\{v\in B_n|\deg_{\sigma(\mathbf{G})\triangle\mathbf{G}}(\sigma(v))\geqslant\frac{2^{n-2}}{n+1}\right\},\\ &\mathbf{V}_-=\left\{v\in B_n|\deg_{\sigma(\mathbf{G})\triangle\mathbf{G}}(\sigma(v))<\frac{2^{n-2}}{n+1}\right\}. \end{aligned}\right\} \tag{46}$$

Заметим, что $|\sigma(\mathbf{G})\triangle\mathbf{G}|\geqslant\frac{1}{2}|\mathbf{V}_+|\cdot 2^{n-2}/n+1$, поэтому

$$|\mathbf{V}_+|\leqslant\frac{n^{-6}2^{2n-25}}{2^{n-3}/(n+1)}=O(n^{-5}2^n)<h<2^{n-1}. \tag{47}$$

Отсюда $|\mathbf{V}_-|>2^{n-1}$; следовательно, линейное замыкание множества $\mathbf{V}_-$ совпадает с B_n и, значит, $\mathbf{V}_-$ содержит некоторый базис $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ пространства B_n. Пусть σ' — линейный эндоморфизм, совпадающий с σ на базисе $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Мы хотим доказать следующий факт:

$$\exists w\in\mathbf{V}_-\left(\deg_{\sigma(G_0)\triangle G_0}(\sigma(w))\geqslant\frac{1}{n+1}\cdot 2^{n-1}\right). \tag{48}$$

Разберем два случая.

Случай 1. $\sigma'|_{\mathbf{V}_-}\neq\sigma|_{\mathbf{V}_-}$.

Пусть $\mathbf{v}\in\mathbf{V}_-$; $\sigma'(\mathbf{v})\neq\sigma(\mathbf{v})$. Разложим $\mathbf{v}$ по базису $\{\mathbf{v}_i\}$: $\mathbf{v}=\bigoplus_{i=1}^{n}\lambda_i\mathbf{v}_i$ $(\lambda_i\in\mathbf{F}_2)$. Тогда $\sigma(\mathbf{v})\neq\bigoplus_{i=1}^{n}\lambda_i\sigma(\mathbf{v}_i)$ и, следовательно, $|\mathbf{H}|=2^{n-1}$, где $\mathbf{H}=\left\{x\,|\,\langle\sigma(\mathbf{v}), x\rangle\neq\bigoplus_{i=1}^{n}\lambda_i\langle\sigma(\mathbf{v}_i), x\rangle\right\}$. Для любого $x\in\mathbf{H}$ выполнено хотя бы одно из неравенств $\langle\sigma(\mathbf{v}), x\rangle\neq\langle\mathbf{v}, \sigma^{-1}(x)\rangle$; $\langle\sigma(\mathbf{v}_i), x\rangle\neq\langle\mathbf{v}_i, \sigma^{-1}(x)\rangle$ $(1\leqslant i\leqslant n)$, т. е. вершина x инцидентна в графе $\sigma(G_0)\triangle G_0$ хотя бы одной из вершин $\sigma(\mathbf{v}), \sigma(\mathbf{v}_1), \ldots, \sigma(\mathbf{v}_n)$. По принципу Дирихле это влечет (48).

Случай 2. $\sigma'|_{\mathbf{V}_-}=\sigma|_{\mathbf{V}_-}$.

В силу (47) имеем $\rho(\sigma, \sigma')\leqslant h$. Так как $\sigma\notin\mathrm{Aut}^*$, то $\sigma\notin\mathrm{Aut}$. Если бы линейный эндоморфизм σ' сохранял скалярное произведение, то он был бы автоморфизмом и лежал бы в Aut вопреки только что доказанному. Следовательно, для некоторых базисных элементов $\mathbf{v}_i$, $\mathbf{v}_j$ имеем $\langle\sigma'(\mathbf{v}_i), \sigma'(\mathbf{v}_j)\rangle\neq\langle\mathbf{v}_i, \mathbf{v}_j\rangle$, откуда $|\mathbf{H}|=2^{n-1}$, где $\mathbf{H}=\{x\,|\,\langle\sigma'(\mathbf{v}_i), \sigma'(x)\rangle\neq\langle\mathbf{v}_i, x\rangle\}$. Поэтому вершина $\sigma'(\mathbf{v}_i)=\sigma(\mathbf{v}_i)$ инцидентна в графе $\sigma(G_0)\triangle G_0$ всем вершинам из $\sigma(\mathbf{H}\setminus\mathbf{V}_+)$ и, в силу (47), вершину $\mathbf{v}_i$ можно взять в качестве w в (48).

Итак, (48) доказано. Из (46), (48), (29) следует, что

$$\exists w\in B_n\left(\deg_{\sigma(K(S(\mathbf{g})))\triangle K(S(\mathbf{g}))}(\sigma(w))\geqslant\frac{1}{n+1}\cdot 2^{n-1}-\frac{1}{n+1}\cdot 2^{n-2}\right),$$

откуда $|S(\mathbf{g})|\geqslant\frac{2^{n-3}}{n+1}$. Таким образом, соотношение $|\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant n^{-6}2^{2n-25}$ при $\sigma\notin\mathrm{Aut}^*$ влечет $|S(\mathbf{g})|\geqslant\frac{2^{n-3}}{n+1}$, откуда

$$\mathbf{P}[\exists\sigma\notin\mathrm{Aut}^*\,|\,\sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant n^{-6}2^{2n-25}]\leqslant$$
$$\leqslant\mathbf{P}\left[|S(\mathbf{g})|\geqslant\frac{2^{n-3}}{n+1}\right]\leqslant\frac{n+1}{2^{n-3}}\,\mathbf{M}[|S(\mathbf{g})|].$$

Аналогично (22) проверяется, что $\mathbf{M}[|S(\mathbf{g})|]=2^{n-l+o(1)}$ и, окончательно,

$$\mathbf{P}[\exists\sigma\notin\mathrm{Aut}^* \mid \sigma(\mathbf{G})\triangle\mathbf{G}|\leqslant n^{-6}2^{2n-25}]=2^{o(1)-1}. \qquad (49)$$

Из (43), (45), (49) следует, что $\mathbf{P}[A'(\mathbf{G})\leqslant n^{-6}2^{2n-26}]<1$. После этого доказательство теоремы завершается обычным образом.

В заключение сформулируем две открытые проблемы. Первая из них состоит в получении результата, аналогичного доказанным в настоящей работе, для следующего свойства графов: $\omega(G_n)=2$; $\omega(\text{со—}G_n)=O(2^{\varepsilon n})$ для некоторой константы $\varepsilon<1$. Неконструктивно доказано существование таких G_n для любых $\varepsilon>\frac{1}{2}$ ([2], с. 25).

Вопрос 1. Существует ли последовательность булевых функций $f_n(x_1,\ldots,x_{2n})$, вычислимая формулами полиномиального размера ограниченной глубины в базисе $\{\&, \oplus\}$ такая, что $\omega(G(f_n))=2$; $\omega(\text{со—}G(f_n))=O(2^{\varepsilon n})$, где $\varepsilon<1$ — некоторая константа?

В формулировках всех теорем 1—7 верхние оценки величины $L_i(f_n)$ можно заменить более слабым заключением «последовательность f_n вычисляется функциональными схемами полиномиального размера».

Вопрос 2. Можно ли для какой-нибудь из теорем 1—7 заменить верхние оценки величины $L_i(f_n)$ на заключение «последовательность f_n лежит в классе P», пусть даже ценой некоторого ухудшения оценок для рассматриваемых комбинаторных характеристик?

Мне бы хотелось поблагодарить С. И. Адяна за внимание к работе и ряд полезных замечаний.

ЛИТЕРАТУРА

1. *Разборов А. А.* Нижние оценки размера схем ограниченной глубины в базисе $\{\&, \oplus\}$. — препринт МИАН СССР, 1986.
2. *Эрдёш П., Спенсер Дж.* Вероятностные методы в комбинаторике. — М.: Мир, 1976.
3. *Chung F. R. K.* A note on constructive methods for Ramsey numbers. — J. Graph Theory 5 (1981), 109—113.
4. *Frankl P. A.* A constructive lower bound for some Ramsey numbers. — Ars Combinatoria 3 (1977), 297—302.
5. *Paterson M. S.* Bounded depth circuits over $\{\oplus, \wedge\}$ — preprint, Warwick University, 1986
6. *Pudlak P., Rödl V.,* Savicky P. Graph Somplexity. — preprint, Czechoslovak Acad. of Sci., 1987.
7. *Smolensky R.* Algebraic methods in the theory of lower bounds for Boolean circuit complexity. — preprint, University of California, 1986.